routine continues to meet the minimum requirements of this part.

(c) A licensee, certificate holder, or other person must update its NRC facility clearance every five years either by submitting a complete Standard Practice Procedures Plan or a certification that the existing plan is fully current to the Division of Security Operations.

[64 FR 15650, Apr. 1, 1999, as amended at 68 FR 41222, July 11, 2003; 68 FR 58823, Oct. 10, 2003; 72 FR 49562, Aug. 28, 2007; 74 FR 62685, Dec. 1, 2009]

§ 95.20 Grant, denial or termination of facility clearance.

The Division of Security Operations shall provide notification in writing (or orally with written confirmation) to the licensee, certificate holder, or other person of the Commission's grant, acceptance of another agency's facility clearance, denial, or termination of facility clearance. This information must also be furnished to representatives of the NRC, NRC contractors, licensees, certificate holders, or other person, or other Federal agencies having a need to transmit classified information to the licensees or other person.

[72 FR 49562, Aug. 28, 2007, as amended at 74 FR 62685, Dec. 1, 2009]

§ 95.21 Withdrawal of requests for facility security clearance.

When a request for facility clearance is to be withdrawn or canceled, the requester shall notify the NRC Division of Security Operations in the most expeditious manner so that processing for this approval may be terminated. The notification must identify the full name of the individual requesting discontinuance, his or her position with the facility, and the full identification of the facility. The requestor shall confirm the telephone notification promptly in writing.

[64 FR 15651, Apr. 1, 1999, as amended at 68 FR 41222, July 11, 2003; 74 FR 62685, Dec. 1, 2009]

§ 95.23 Termination of facility clearance.

(a) Facility clearance will be terminated when—

(1) There is no longer a need to use, process, store, reproduce, transmit, transport or handle classified matter at the facility; or

(2) The Commission makes a determination that continued facility clearance is not in the interest of national security.

(b) When facility clearance is terminated, the licensee, certificate holder, or other person will be notified in writing of the determination and the procedures outlined in § 95.53 apply.

[62 FR 17692, Apr. 11, 1997, as amended at 72 FR 49562, Aug. 28, 2007]

§ 95.25 Protection of National Security Information and Restricted Data in storage.

(a) Secret matter, while unattended or not in actual use, must be stored in—

(1) A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours; or

(2) Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets, or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar must be secured to the cabinet by welding, rivets, or bolts, so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container must be held securely so their contents cannot be removed without forcing open the drawer. This type of cabinet will be accorded supplemental protection during non-working hours.

(b) Confidential matter while unattended or not in use must be stored in the same manner as SECRET matter except that no supplemental protection is required.

(c) *Classified lock combinations.* (1) A minimum number of authorized persons may know the combinations to authorized storage containers. Security containers, vaults, cabinets, and other authorized storage containers must be kept locked when not under

the direct supervision of an authorized person entrusted with the contents.

(2) Combinations must be changed by a person authorized access to the contents of the container, by the Facility Security Officer, or his or her designee.

(d) *Records of combinations.* If a record is made of a combination, the record must be marked with the highest classification of material authorized for storage in the container. Superseded combinations must be destroyed.

(e) *Selections of combinations.* Each combination must be randomly selected and require the use of at least three different numbers. In selecting combinations, multiples, simple arithmetical ascending or descending series, telephone numbers, social security numbers, car license numbers, and calendar dates such as birthdates and anniversaries, shall be avoided.

(f) Combinations will be changed only by persons authorized access to Secret or Confidential National Security Information and/or Restricted Data depending upon the matter authorized to be stored in the security container.

(g) *Posted information.* Containers may not bear external markings indicating the level of classified matter authorized for storage. A record of the names of persons having knowledge of the combination must be posted inside the container.

(h) *End of day security checks.* (1) Facilities that store classified matter shall establish a system of security checks at the close of each working day to ensure that all classified matter and security repositories have been appropriately secured.

(2) Facilities operating with multiple work shifts shall perform the security checks at the end of the last working shift in which classified matter had been removed from storage for use. The checks are not required during continuous 24-hour operations.

(i) *Unattended security container found opened.* If an unattended security container housing classified matter is found unlocked, the custodian or an alternate must be notified immediately. Also, the container must be secured by protective personnel. An effort must be made to determine if the contents were compromised not later than the next day.

(j) *Supervision of keys and padlocks.* Use of key-operated padlocks are subject to the following requirements:

(1) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified matter;

(2) A key and lock control register must be maintained to identify keys for each lock and their current location and custody;

(3) Keys and locks must be audited each month;

(4) Keys must be inventoried with each change of custody;

(5) Keys must not be removed from the premises;

(6) Keys and spare locks must be protected equivalent to the level of classified matter involved;

(7) Locks must be changed or rotated at least every 12 months, and must be replaced after loss or compromise of their operable keys; and

(8) Master keys may not be made.

[45 FR 14483, Mar. 5, 1980, as amended at 47 FR 9196, Mar. 4, 1982; 50 FR 36985, Sept. 11, 1985; 53 FR 19263, May 27, 1988; 59 FR 48975, Sept. 23, 1994; 62 FR 17693, Apr. 11, 1997; 64 FR 15651, Apr. 1, 1999]

§ 95.27 Protection while in use.

While in use, classified matter must be under the direct control of an authorized individual to preclude physical, audio, and visual access by persons who do not have the prescribed access authorization or other written CSA disclosure authorization (see § 95.36 for additional information concerning disclosure authorizations).

[64 FR 15651, Apr. 1, 1999]

§ 95.29 Establishment of Restricted or Closed areas.

(a) If, because of its nature, sensitivity or importance, classified matter cannot otherwise be effectively controlled in accordance with the provisions of §§ 95.25 and 95.27, a Restricted or Closed area must be established to protect this matter.

(b) The following measures apply to Restricted Areas:

(1) Restricted areas must be separated from adjacent areas by a physical